On the congruences $a^n \pm b^n \equiv 0 \bmod n^k$

Salvatore Tringali

Abstract. We determine all triples (a, b, n) of integers with $\gcd(a, b) = 1$ and $n \ge 1$ such that n^k divides $a^n + b^n$ for $k = \max(|a|, |b|)$. In particular, for positive integers m, n we show that $n^m \mid m^n + 1$ if and only if either $(m, n) = (2, 3)$, $(m, n) = (1, 2)$, or $n = 1$ and m is arbitrary; this generalizes a couple of problems from the 1990 and 1999 editions of the International Mathematical Olympiad. Then we solve the same question with $a^n - b^n$ in place of $a^n + b^n$. The results are related to a conjecture by K. Győry and C. Smyth on the finiteness of $\{n \in \mathbb{N}^+ : n^k \mid a^n \pm b^n\}$ when a, b, k are fixed integers with $k \ge 3$, $\gcd(a, b) = 1$, and $|a|, |b|$ not simultaneously equal to 1.

Keywords. Congruences, exponential Diophantine equations.

2010 Mathematics Subject Classification. Primary 11A07, 11A99.

1 Introduction

It is a problem from the 1990 edition of the International Mathematical Olympiad (shortly, IMO) to find all integers $n \ge 2$ such that $n^2 \mid 2^n + 1$. This is reported as Problem 7.1.15 (p. 147) in [1], together with a solution by the authors (p. 323), which shows that the only possible n is 3. On another hand, Problem 4 in the 1999 IMO asks to list all pairs (n, p) of positive integers such that p is a (positive rational) prime, $n \le 2p$ and $n^{p-1} \mid (p-1)^n + 1$. This is Problem 5.1.3 (p. 105) in the same book as above, whose solution by the authors (p. 105) is concluded with the remark that "With a little bit more work, we can even erase the condition $n \le 2p$." Specifically, it is found that the required pairs are $(1, p)$, $(2, 2)$ and $(3, 3)$, where p is an arbitrary prime.

It is now fairly natural to ask whether similar conclusions can be drawn in relation to the more general problem of determining all pairs (m, n) of positive integers for which $n^m \mid m^n + 1$. In fact, the question is answered in the positive, and even in a stronger form, by the following proposition, which represents the main contribution of the present paper:

The author is funded from the European Community's 7th Framework Programme (FP7/2007-2013) under Grant Agreement No. 276487 (project ApProCEM).

Proposition 1.1. *Let a, b, n be integers with* $\gcd(a, b) = 1$ *and* $n \ge 1$. *Then* n^k *divides* $a^n + b^n$ *for* $k = \max(|a|, |b|)$ *if and only if either of the following holds:*

(i) a, b *are any coprime integers and* $n = 1$.

(ii) $a, b \in \{\pm 1\}$ *and* $n = 2$.

(iii) $(a, b) = (\varepsilon, -\varepsilon)$ *for* $\varepsilon \in \{\pm 1\}$ *and* n *is any positive odd integer* ≥ 3.

(iv) $(a, b, n) = (2\varepsilon, \varepsilon, 3)$ *or* $(a, b, n) = (\varepsilon, 2\varepsilon, 3)$ *for* $\varepsilon \in \{\pm 1\}$.

Proposition 1.1 is proved in Section 2. For what it is worth, let us be explicit and observe, with the notation as in the above statement, that the result yields a solution of the IMO problems which have originally stimulated this work in the case where $a \ge 1$ and $b = 1$. More specifically, the next corollary is immediate (we omit the obvious proof):

Corollary. *Let* $m, n \in \mathbb{N}^+$. *Then* $n^m \mid m^n + 1$ *if and only if either* $(m, n) = (2, 3)$, $(m, n) = (1, 2)$, *or* $n = 1$ *and* m *is arbitrary.*

Also, we use Proposition 1.1 to prove the following:

Proposition 1.2. *Let a, b, n be integers with* $\gcd(a, b) = 1$ *and* $n \ge 1$. *Then* n^k *divides* $a^n - b^n$ *for* $k = \max(|a|, |b|)$ *if and only if either of the following holds:*

(i) a, b *are any coprime integers and* $n = 1$.

(ii) $a, b \in \{\pm 1\}$ *and* n *is any positive even integer.*

(iii) $(a, b) = (\varepsilon, \varepsilon)$ *for* $\varepsilon \in \{\pm 1\}$ *and* n *is any positive odd integer* ≥ 3.

(iv) $(a, b, n) = (3\varepsilon_1, \varepsilon_2, 2)$ *or* $(a, b, n) = (\varepsilon_1, 3\varepsilon_2, 2)$ *for* $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$.

(v) $(a, b, n) = (2\varepsilon, -\varepsilon, 3)$ *or* $(a, b, n) = (-\varepsilon, 2\varepsilon, 3)$ *for* $\varepsilon \in \{\pm 1\}$.

For the notation and terminology used throughout but not defined, as well as for material concerning classical topics in number theory, the reader should refer to [5]. In particular, we write $\mathbb{R}$ for the ordered field of real numbers, $\mathbb{P}$ for the set of all (positive rational) primes, $\mathbb{Z}$ for the ordered ring of integers, $\mathbb{N}$ for the subsemiring of $\mathbb{Z}$ of nonnegative integers, and $\mathbb{N}^+$ for $\mathbb{N} \setminus \{0\}$. For $a, b \in \mathbb{Z}$ we denote by $\gcd(a, b)$ the greatest common divisor of a and b if $a^2 + b^2 \ne 0$, and we set $\gcd(a, b) := \infty$ otherwise. Lastly, for $c \in \mathbb{Z} \setminus \{0\}$ and $p \in \mathbb{P}$ we use $e_p(c)$ to mean the greatest exponent $k \in \mathbb{N}$ such that $p^k \mid c$, while we let $e_p(0) := \infty$.

We will make use at some point of the following result, which belongs to the folklore and is typically attributed to É. Lucas [6] and R.D. Carmichael [3] (the latter having fixed an error in Lucas' original work in the 2-adic case).

Lemma 1.3 (Lifting-the-exponent lemma). *For all $x, y \in \mathbb{Z}$, $\ell \in \mathbb{N}^+$ and $p \in \mathbb{P}$ such that $p \nmid xy$ and $p \mid x - y$, the following conditions are satisfied:*

(i) *If $p \geq 3$, ℓ is odd, or $4 \mid x - y$, then $e_p(x^\ell - y^\ell) = e_p(x - y) + e_p(\ell)$.*

(ii) *If $p = 2$, ℓ is even and $e_2(x - y) = 1$, then $e_2(x^\ell - y^\ell) = e_2(x + y) + e_2(\ell)$.*

In fact, our proof of Proposition 1.1 is but the result of a meticulous refinement of the solutions already known for the problems mentioned in the preamble. Hence, our only possible merit, if any at all, has been that of bringing into focus a clearer picture of (some of) their essential issues.

The study of the congruences $a^n \pm b^n \equiv 0 \bmod n^k$ has a very long history, dating back at least to Euler, who proved that, for all integers a, b with $\gcd(a, b) = 1$ and $a > b \geq 1$, every primitive prime divisor of $a^n - b^n$ is congruent to 1 modulo n; see [2, Theorem I] for a proof and [2, §1] for the terminology. However, since there are so many results related to the question, instead of trying to summarize them, we just refer the reader to the paper [4], whose authors provide an account of the existing literature on the topic. The paper also characterizes, for fixed $a, b \in \mathbb{Z}$ and $k \in \mathbb{N}^+$, the sets $R_k^+(a, b)$, respectively $R_k^-(a, b)$, of all positive integers n such that n^k divides $a^n + b^n$, respectively $a^n - b^n$ (note that no assumption is made about the coprimality of a and b), and addresses the problem of finding the exceptional cases when $R_1^-(a, b)$ and $R_2^-(a, b)$ are finite; see, in particular, [4, Theorems 1–2 and 18]. Nevertheless, the related problem of determining, for fixed $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, all positive integers n such that n^k divides $a^n + b^n$ (respectively, $a^n - b^n$) for $k = \max(|a|, |b|)$ does not appear to be considered neither in [4] nor in the references therein.

On another hand, it is suggested in [4] that $R_k^+(a, b)$ and $R_k^-(a, b)$ are both finite provided that a, b, k are fixed integers with $k \geq 3$, and $|a|, |b|$ are relatively prime but not simultaneously equal to 1; the authors point out that the question is probably a difficult one, even assuming the ABC conjecture. Although far from providing an answer, Propositions 1.1 and 1.2 in the present paper prove in this respect that, under the same assumptions, $R_k^+(a, b)$ and $R_k^-(a, b)$ are finite for all sufficiently large k, and indeed for $k \geq \max(|a|, |b|)$.

2 Proofs

For the sake of exposition, we premise a couple of lemmas.

Lemma 2.1. *Let $x, y, z \in \mathbb{Z}$ and $\ell \in \mathbb{N}^+$ such that $\gcd(x, y) = 1$ and $z \mid x^\ell + y^\ell$. Then xy and z are relatively prime, $q \nmid x^\ell - y^\ell$ for every integer $q \geq 3$ for which $q \mid z$, and $4 \nmid z$ provided that ℓ is even. Moreover, if there exists an odd prime* *divisor p of z and ℓ such that* $\gcd(\ell, p-1) = 1$*, then* $p \mid x+y$*,* ℓ *is odd and* $e_p(z) \le e_p(x+y) + e_p(\ell)$*.*

Proof. The first part is routine (we omit the details). As for the second, let p be an odd prime dividing both z and ℓ with $\gcd(\ell, p-1) = 1$; also, considering that z and xy are relatively prime (by the above), denote by y^{-1} an inverse of y modulo p and by ω the order of xy^{-1} modulo p, viz the smallest $k \in \mathbb{N}^+$ such that $(xy^{-1})^k \equiv 1 \bmod p$; cf. [5, §6.8]. Since $(xy^{-1})^{2\ell} \equiv 1 \bmod p$, we have $\omega \mid 2\ell$. It follows from Fermat's little theorem and [5, Theorem 88] that ω divides $\gcd(2\ell, p-1)$, whence we get $\omega \mid 2$, using that $\gcd(\ell, p-1) = 1$. This in turn implies that $p \mid x^2 - y^2$, to the effect that either $p \mid x-y$ or $p \mid x+y$. But $p \mid x-y$ would give that $p \mid x^\ell - y^\ell$, which is however impossible by the first part of the claim (since $p \ge 3$). So $p \mid x+y$, with the result that ℓ is odd: For if $2 \mid \ell$ then $p \mid 2x^\ell$ (because $p \mid z \mid x^\ell + y^\ell$ and $y \equiv -x \bmod p$), which would lead to $\gcd(x,y) \ge p$ (again, using that p is odd), that is to a contradiction. The rest is an immediate application of Lemma 1.3. □

Lemma 2.2. *Let* $x, y, z \in \mathbb{Z}$ *such that* x, y *are odd. Then* $x^2 - y^2 = 2^z$ *if and only if* $z \ge 3$*,* $x = (2^{z-2}+1)\varepsilon_1$ *and* $y = (2^{z-2}-1)\varepsilon_2$ *with* $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$*.*

Proof. Since x and y are odd, $x^2 - y^2$ is divisible by 8, i.e. $z \ge 3$, and there exist $i, j \in \mathbb{N}^+$ and $\varepsilon \in \{\pm 1\}$ such that $i + j = z$, $x - y = 2^i\varepsilon$ and $x + y = 2^j\varepsilon$. It follows that $x = (2^{j-1} + 2^{i-1})\varepsilon$ and $y = (2^{j-1} - 2^{i-1})\varepsilon$, and then either $i = 1$ or $j = 1$ (otherwise x and y would be even). The rest is straightforward. □

We are ready to write down the proof of our main results.

Proof of Proposition 1.1. Let us suppose (by symmetry) that $|a| \ge |b|$ and $n^{|a|}$ divides $a^n + b^n$. The case $n = 1$ is trivial, so we assume $n \ge 2$. Since on the one hand a and b are relatively prime, while on the other hand $n \nmid a^n + b^n$ if $|a| = 1$ and $b = 0$, we then have $|a| \ge |b| \ge 1$. The case $|a| = 1$ is trivial too, and leads to points (ii) and (iii) in our claim. Hence, we suppose in the sequel that

$$|a| \ge 2 \quad \text{and} \quad |a| > |b| \ge 1. \tag{1}$$

Considering that $4 \mid n^2$ whenever $2 \mid n$, it follows from Lemma 2.1 that n is odd and $\gcd(ab, n) = 1$. Denote by p the smallest prime divisor of n. Again by Lemma 2.1, it is found that $p \mid a + b$ and

$$|a| - 1 \le (|a| - 1)e_p(n) \le e_p(a+b). \tag{2}$$

Also, $a + b \neq 0$ by equation (1), with the result that

$$a + b = p^r s, \quad \text{with } r \in \mathbb{N}^+, s \in \mathbb{Z} \setminus \{0\} \text{ and } p \nmid s. \tag{3}$$

Then, equations (1) and (3) yield that $2|a| \geq p^r \cdot |s| + 1$. This implies by equation (2), since $r = e_p(a + b)$, that

$$3^r \cdot |s| \leq p^r \cdot |s| \leq 2r + 1,$$

which is possible only if $p = 3$ and $r = |s| = 1$. So, by equations (2) and (3), $|a + b| = 3$ and $|a| = 2$, to the effect that either $(a, b) = (2, 1)$ or $(a, b) = (-2, -1)$. Furthermore, $e_3(n) = 1$, and hence $n = 3t$ for some $t \in \mathbb{N}^+$ with $\gcd(6, t) = 1$. It follows that $t^2 \mid \alpha^t + 1$ for $\alpha = 2^3$.

Suppose by contradiction that $t \geq 2$ and let q be the least prime divisor of t. Then another application of Lemma 2.1 gives $2e_q(t) \leq e_q(\alpha + 1) + e_q(t)$, and accordingly $1 \leq e_q(t) \leq e_q(\alpha + 1) = e_q(3^2)$, which is however absurd due to the fact that $\gcd(3, t) = 1$. Therefore $t = 1$, i.e. $n = 3$, and putting all together completes the proof (once checked that $3^2 \mid 2^3 + 1^3$). □

Proof of Proposition 1.2. The case $n = 1$ is trivial, so suppose in the sequel that $n \geq 2$. Since $n \mid a^n - b^n$ and $\gcd(a, b) = 1$, this gives in the first place $ab \neq 0$; secondly, $|a| = |b|$ only if $a, b \in \{\pm 1\}$, and then if and only if either $a, b \in \{\pm 1\}$ and n is any even positive integer, or $(a, b) = (\varepsilon, \varepsilon)$ for $\varepsilon \in \{\pm 1\}$ and n is any odd integer ≥ 3. Then by symmetry, we also assume for the remainder of the proof that $|a|$ is greater than $|b|$, so that (to summarize)

$$|a| > |b| \geq 1, \quad n \geq 2, \quad \text{and} \quad n^{|a|} \text{ divides } a^n - b^n. \tag{4}$$

With this in hand, write n as $2^r s$, where $r \in \mathbb{N}$, $s \in \mathbb{N}^+$ and $\gcd(2, s) = 1$. Then, equation (4) implies that $\alpha^s + \beta^s$ is divided by $s^{|a|}$ for $\alpha := a^{2^r}$ and $\beta := -b^{2^r}$ (note that $|\alpha| \geq |\beta|$ since $|a| > |b|$), which leads, by Proposition 1.1, to one of the following three cases.

CASE 1: $s = 1$, viz $n = 2^r$ with $r \in \mathbb{N}^+$. Obviously, n is even, and we get (by coprimality) that both a and b are odd, that is $8 \mid a^2 - b^2$. It follows from point (i) of Lemma 1.3 that

$$e_2(a^{2^r} - b^{2^r}) = e_2(a^2 - b^2) + e_2(2^{r-1}) = e_2(a^2 - b^2) + r - 1.$$

(We apply Lemma 1.3 with $x = a^2$, $y = b^2$, $\ell = 2^{r-1}$ and $p = 2$, where the notation is the same as in the statement of the lemma). Since $(2^r)^{|a|}$ divides $a^{2^r} - b^{2^r}$ in view of equation (4) and our standing assumptions, then

$$(|a| - 1) \cdot r \leq e_2(a^2 - b^2) - 1. \tag{5}$$

Now, there exist $u, v \in \mathbb{N}^+$ with $u \geq 2$ and $\gcd(2, v) = 1$ such that $a^2 - b^2 = 2^{u+1}v$, with the result that $|a| > 2^{u/2}\sqrt{v}$. Hence, we get by equation (5), also taking into account that $2^x \geq x + 1$ for every $x \in \mathbb{R}$ with $x \geq 1$, that

$$\left(\frac{u}{2} + 1\right)\sqrt{v} \leq 2^{u/2}\sqrt{v} < \frac{u}{r} + 1, \tag{6}$$

which is possible only if $r = 1$ and $\sqrt{v} < 2$. Then $2^{u/2}\sqrt{v} < u + 1$, with the result that $2 \leq u \leq 5$ and $v = 1$ (using that v is odd). In the light of Lemma 2.2, all of this implies, in the end, that the conditions in equation (4), when n is a positive power of two, are satisfied only if $a = (2^z + 1)\varepsilon_1$, $b = (2^z - 1)\varepsilon_2$ and $n = 2$, where $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ and z is an integer between 1 and 4; but now we need $2^z \leq z + 1$ by equation (5), so necessarily $z = 1$, i.e. $a = 3\varepsilon_1$ and $b = \varepsilon_2$ (and, in fact, $2^3 \mid 3^2 - 1^2$).

Case 2: s is a positive odd integer ≥ 3 and $(\alpha, \beta) = (\varepsilon, -\varepsilon)$ for $\varepsilon \in \{\pm 1\}$. Then $a^{2^r} = \varepsilon$, which is impossible because $|a| \geq 2$ by equation (4).

Case 3: $(\alpha, \beta, s) = (2\varepsilon, \varepsilon, 3)$ for $\varepsilon \in \{\pm 1\}$ (recall that $|\alpha| \geq |\beta|$). Then $a^{2^r} = 2\varepsilon$ and $b^{2^r} = -\varepsilon$, to the effect that $r = 0$, and hence $(a, b, n) = (2\varepsilon, -\varepsilon, 3)$ for $\varepsilon \in \{\pm 1\}$.

Putting all the pieces together, the proof is thus complete. □

Acknowledgments. I am grateful to Paolo Leonetti (Università Bocconi di Milano) for useful discussions, and to Carlo Sanna (Università di Torino) for his careful proofreading and for providing remarks that improved the readability of the paper.

Bibliography

[1] T. Andreescu and D. Andrica, *Number Theory - Structures, Examples, and Problems*, 1st ed., Birkhäuser, 2009.

[2] G. D. Birkhoff and H. S. Vandiver, On the Integral Divisors of $a^n - b^n$, *Ann. of Math.*, 2nd Series, **5**, 4 (Jul., 1904), 173–180.

[3] R. D. Carmichael, On the Numerical Factors of Certain Arithmetic Forms, *Amer. Math. Monthly*, **16**, 10 (1909), 153–159.

[4] K. Győry and C. Smyth, The divisibility of $a^n - b^n$ by powers of n, *Integers*, **10**, 3 (Jul., 2010), 319–334.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 6th ed. (revised by D.R. Heath-Brown and J.H. Silverman), Oxford University Press, 2008.

[6] É. Lucas, Théorie des Fonctions Numériques Simplement Periodiques, *Amer. J. Math*, **1** (1878), 184–196, 197-240, 289–321.

Author information

Salvatore Tringali, Laboratoire Jacques-Louis Lions (LJLL), Institut de Mathématiques de Jussieu (IMJ), Université Pierre et Marie Curie (UPMC), 4 place Jussieu, boîte courrier 187, 75252 Paris (cedex 05), France.
E-mail: `tringali@ann.jussieu.fr`